Cite this paper as: Armandi, M. & Ranjbarfard, M., (2018), “Ranking of effective factors in evaluating the information security of the organization based on the international standard ISO 27001”, *3rd International Conference on Applied Researches in Science & Engineering 5th January 2018 - Istanbul Turkey Marmara University*

# Ranking of effective factors in evaluating the information security of the organization based on the international standard ISO 27001

**Melika Armandi, Mina Ranjbarfard[1]**

*Department of management, Alzahra University, Tehran, Iran*

**Abstract:**

Today, information is considered as a vital element for the survival of the organization and information security is a significant issue in organizations. To achieve an acceptable level of security, organizations can use successful global methods and standards in this area. Using standards can help managers make the right decisions in this area. The standard control framework should have comprehensive control objectives to deal with threats. Loss of any of these dimensions undermines the organization's ability to deal with unwanted threats. According to experts the importance of these goals and criteria is not the same, and some have a higher priority than others. In this paper, the control targets of ISO 27001 are ranked using the Demetel technique and the cause-and-effect relationship between them is investigated. Also, the ranking of security evaluation criteria is done with the VASPAS technique. This technique is a combination of two methods of total weight model and weight product model and has a higher accuracy than independent models. The results of this article can be used in the process of information security audit and based on the obtained ranking can be applied to create and modify a secure structure in the organization.

**Keywords:** Information Security, Information Security Standard, ISO 27001, Demetel Technique, VASPAS Technique

[1] m.ranjbarfard@alzahra.ac.ir



3rd International Conference on Applied Researches in Science & Engineering

5th January 2018 - Istanbul Turkey

Marmara University



# رتبه‌بندی عوامل تأثیرگذار در ارزیابی امنیت اطلاعات سازمان مبتنی بر استاندارد بین‌المللی ایزو ۲۷۰۰۱

**ملیکا ارمندئی[۱]*، مینا رنجبرفرد[۲]،**

۱- دانشجوی کارشناسی ارشد رشته مدیریت فناوری اطلاعات دانشگاه الزهرا (س)، melikaarmandi@yahoo.com

۲- استادیار گروه مدیریت فناوری اطلاعات دانشگاه الزهرا (س)، mina.ranjbar.ie@gmail.com

## چکیده

امروزه اطلاعات به‌عنوان یک عنصر حیاتی برای بقای سازمان و امنیت اطلاعات به‌عنوان یک موضوع قابل‌توجه در سازمان‌ها مطرح می‌شود. برای دستیابی به سطح امنیتی قابل‌قبول، سازمان‌ها می‌توانند از به روش‌ها و استانداردهای موفق جهانی در این زمینه بهره گیرند. بهره‌گیری از استانداردها می‌تواند مدیران را در تصمیم‌گیری درست در این زمینه یاری رساند. چارچوب کنترل استاندارد باید اهداف کنترلی جامعی برای مقابله با تهدیدات داشته باشد. از دست دادن هرکدام از این ابعاد توانایی سازمان برای مقابله با تهدیدهای ناخواسته را تضعیف می‌کند. میزان اهمیت این اهداف و معیارها طبق نظر خبرگان یکسان نبوده و برخی از اولویت بالاتری نسبت به بقیه برخوردار هستند. در این مقاله، اهداف کنترلی استاندارد ایزو ۲۷۰۰۱ با استفاده از تکنیک دیمتل رتبه‌بندی می‌شوند و رابطه علت و معلولی میان آنها بررسی می‌شود. همچنین رتبه‌بندی معیارهای ارزیابی امنیت با تکنیک واسپاس انجام می‌شود. این تکنیک، ترکیبی از دو روش مدل مجموع وزنی و مدل محصول وزنی می‌باشد و نسبت به مدل‌های مستقل از دقت بالاتری برخوردار است. از نتایج این مقاله می‌توان در فرآیند ممیزی امنیت اطلاعات استفاده نمود و بر مبنای رتبه‌بندی به‌دست‌آمده به ایجاد و اصلاح ساختار امن در سازمان پرداخت.

**واژه‌های کلیدی:** امنیت اطلاعات، استاندارد امنیت اطلاعات، ایزو ۲۷۰۰۱، تکنیک دیمتل، تکنیک واسپاس

### ۱- مقدمه

در حال حاضر تهدید به امنیت اطلاعات یک مسئله جهانی است اما با این وجود هنوز اطلاعات و دانش کافی برای پیش‌بینی و کاهش اثرات آن در بسیاری از سازمان‌ها وجود ندارد [۱]. ایجاد یک محیط ایمن در سازمان‌های مدرن اطلاعاتی یکی از چالش‌های اساسی در عصر حاضر محسوب می‌گردد. برای بسیاری از سازمان‌ها و مؤسسات اهمیت و ضرورت توجه جدی به مقوله امنیت اطلاعات هنوز در هاله‌ای از ابهام قرار دارد و برخی دیگر امنیت را تا سطح یک محصول تنزل داده و فکر می‌کنند که با تهیه یک محصول نرم‌افزاری خاص و نصب آن در سازمان خود، امنیت را برای سازمان خود به ارمغان می‌آورند [۲]. استانداردها به‌روش‌های بسیاری در زمینه امنیت اطلاعات تدوین شده‌اند که زمینه مناسبی برای بهره‌گیری از رویکرد حفاظت سازمانی فراهم کرده‌اند و به سازمان‌ها کمک می‌کنند تا با پیاده‌سازی و استقرار سیستم مدیریت امنیت اطلاعات فرآیندهای امنیتی خود را متناسب با الزامات خویش به نحو مطلوبی بهبود ببخشند. پس از پیاده‌سازی سیستم مدیریت امنیت اطلاعات انطباق آن با کنترل‌ها و الزامات استاندارد بررسی می‌شود تا از کارایی هر چه بهتر و بهبود مستمر این سیستم اطمینان حاصل شود [۳]. میزان اهمیت کنترل‌ها و الزامات در تمامی استانداردهای مدیریت امنیت اطلاعات یکسان در نظر گرفته شده است، در صورتی که طبق نظر خبرگان تأثیر این معیارها در برقراری سطح امنیتی مطلوب یکسان نمی‌باشد. راه‌حلی که این پژوهش در این حیطه پیشنهاد می‌کند، رتبه‌بندی و تعیین اولویت اهداف و معیارهای ارزیابی استاندارد مدیریت امنیت اطلاعات برای بررسی تأثیر واقعی این عوامل در برقراری امنیت اطلاعات سازمان می‌باشد.

## ۲- مبانی نظری تحقیق

### ۲-۱- مفهوم سیستم مدیریت امنیت اطلاعات

سیستم مدیریت امنیت اطلاعات، اولین بار طی مراحل تحریر و توسعه استاندارد بریتانیایی BS7799 در سال‌های انتهایی ۱۹۸۰ میلادی موردبحث و توجه قرار گرفت. آخرین تعریف سیستم مدیریت امنیت اطلاعات از نظر استاندارد بین‌المللی آن عبارت است از: سیستم مدیریت امنیت اطلاعات بخشی از سیستم مدیریت کلی و سراسری در یک سازمان است که بر پایه رویکرد مخاطرات کسب‌وکار قرار داشته و هدف آن، پایه‌گذاری، بهره‌برداری، نظارت، بازبینی، نگهداری و بهبود امنیت اطلاعات است [۴]. سیستم مدیریت امنیت اطلاعات یک سیستم جامع امنیتی است که بر پایه سه اصل اساسی بنا شده است، این اصول عبارت‌اند از:

سیاست‌ها و دستورالعمل‌های امنیتی: طرح‌ها و برنامه‌های مرتبط برای نحوه محافظت از سیستم‌های اطلاعاتی و داده‌های آن‌ها که در این بخش به آن‌ها پرداخته‌شده است.

استراتژی‌های امنیتی در دو بخش فنی و غیر فنی ارائه‌شده که بخش غیر فنی شامل تعیین سطوح امنیتی مطلوب و انتخاب استانداردهای امنیتی و بخش فنی شامل دستورالعمل‌های لازم برای به‌کارگیری و نظارت بر اجزای سیستم امنیتی جهت نیل به اهداف استراتژیک امنیتی می‌باشد.

تکنولوژی و محصولات امنیتی: این قسمت شامل تمام ابزارهای مورداستفاده در بخش‌های مختلف امنیتی برای اعمال دستورالعمل‌ها، کنترل و پایش می‌باشد.

عوامل اجرایی: شامل افراد مرتبط با مدیریت و اجرای سیستم امنیتی شامل مدیران سیستم‌ها و شبکه‌ها، کارکنان و کاربران عادی می‌باشد. این افراد از تکنولوژی و محصولات امنیتی در جهت سیاست‌ها و دستورالعمل‌های امنیتی استفاده می‌کنند [۴].

## ۲-۲- استانداردهای مدیریت امنیت اطلاعات

استانداردهای مدیریت امنیت اطلاعات یک چارچوب امنیتی همراه با فن‌های تخصصی برای پیاده‌سازی امنیت در فضای تبادل اطلاعات فراهم می‌کنند. استانداردهای جهانی مختلفی در زمینه فناوری اطلاعات و ارتباطات وجود دارد که منجر به امنیت اطلاعات می‌شوند، مانند:BS 7799 ، ISO/IEC27001/2، NIST 800-53 CFS، CIS، ISACA COBIT، ISF، DISA، ITIL، PCI-DSS، OWASP، BSIMM، CSA4، ILTAT، COSO، SOA، OPM و غیره؛ برخی از این استانداردها به دلایل مختلف چندان مورد استقبال سازمان‌ها قرار نگرفته است. در این مقاله با توجه به نظرسنجی‌های انجام شده در سایت جهانی iso.org به بررسی پنج استاندارد امنیت برتر دنیا پرداخته شده است که به‌طور گسترده درزمینه چارچوب، ساختار و امنیت فناوری اطلاعات مورداستفاده قرار می‌گیرند. این پنج استاندارد برتر شامل استاندارد مدیریتی ISO/IEC27001 از موسسه بین‌المللی استاندارد، استاندارد COBIT از موسسه دولتی فناوری اطلاعات، کتابخانه زیرساخت فناوری اطلاعات (ITIL)، استاندارد BS 7799 از موسسه ملی استاندارد انگلستان و PCI-DSS هستند.

## ۳-۲- مقایسه پنج استاندارد برتر

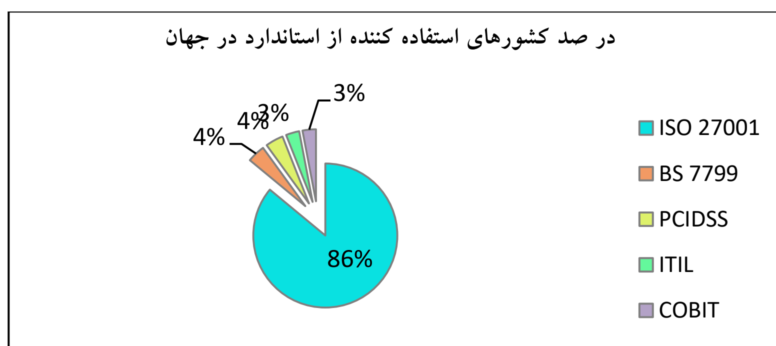
به‌زعم دو تن از محققان حوزه امنیت اطلاعات، استانداردهای موجود در حوزه امنیت اطلاعات در دودسته جای می‌گیرند:

- استانداردهایی که در ایالات‌متحده ایجاد شده و مورداستفاده قرار می‌گیرند. COBIT و ITIL جز این دسته هستند.
- استانداردهایی که در اروپا توسعه داده‌شده و مورداستفاده قرارگرفته‌اند.ISO/IEC 27001 و BS7799 جز این دسته محسوب می‌شود.

استانداردهای اروپایی می‌توانند توسط مراجع تائید شده همانند ISO و BSI مورد ممیزی قرار بگیرند و سازمان‌های مورد تائید موفق به اخذ گواهینامه معتبر شوند اما استانداردهای آمریکایی به‌عنوان یک راهنمای خود ارزیاب مورداستفاده قرار می‌گیرند و گواهینامه‌ای به سازمانی که استاندارد را پیاده‌سازی کرده تعلق نمی‌گیرد [۵]. والهاف معتقد است COBIT و ITIL چارچوب‌هایی هستند که به‌طور گسترده‌تر به بحث تضمین ارائه خدمات فن‌آوری اطلاعات مربوط می‌شوند. آخرین نسخه ITIL به‌خوبی کلیه فرآیندها و مفاهیمی که در یک سازمان برای ارائه خدمات فن‌آوری اطلاعات وجود دارد را توصیف کرده و پوشش می‌دهند و COBIT به‌خوبی کنترل و سنجه‌ها را معرفی می‌نماید؛ اما هنگامی‌که راجع به امنیت اطلاعات صحبت می‌شود هیچ‌کدام از این چارچوب‌ها کافی نبوده و نتوانسته‌اند تمام س را پوشش دهند و استاندارد ISO/IEC 27001 توانسته شکل کاملی از فرآیندها و کنترل‌های امنیتی را برای سازمان فراهم آورد [۵].

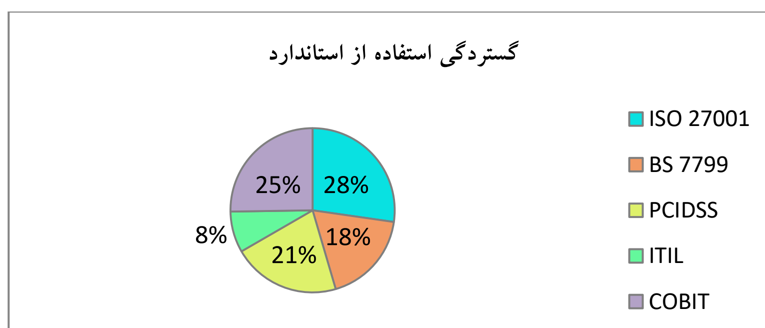
## ۴-۲- انتخاب استاندارد جهت طراحی سیستم خبره امنیت اطلاعات

چارچوب کنترل استاندارد باید اهداف کنترلی جامعی برای مقابله با تهدیدات داشته باشد. طراحی اهداف جامع کنترلی باید به تفکیک وظایف و دانش لازم برای اجرای آن انجام گیرد. از دست دادن هرکدام از این ابعاد توانایی شما برای مقابله با تهدیدهای ناخواسته را تضعیف می‌کند [۶]. سوسانتو و همکاران در پژوهشی که در سال ۲۰۱۵ انجام داده‌اند به مقایسه استانداردهای نامبرده از ابعاد گوناگونی پرداخته‌اند: شکل ۱ درصد کشورهای استفاده کننده از پنج استاندارد برتر در سطح جهان نسبت به یکدیگر را نشان می‌دهد:




**شکل ۱: درصد کشورهای استفاده کننده از استاندارد در جهان** [۷]

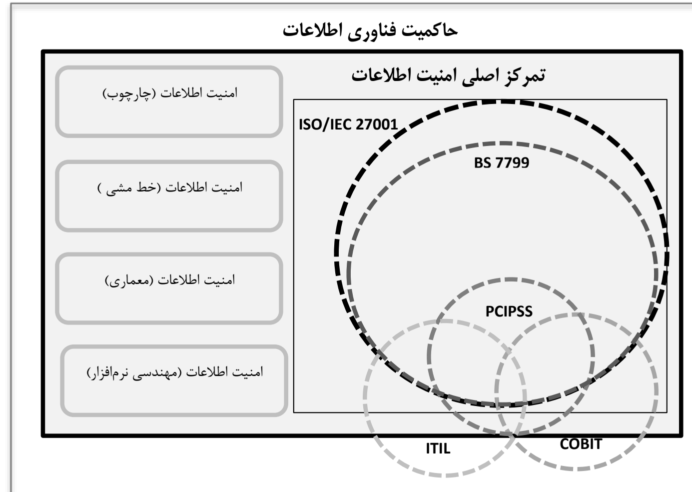
گستردگی استفاده از استانداردها نیز در مقایسه با هم در شکل ۲ نشان داده شده است:




**شکل ۲: گستردگی استفاده از استاندارد در سطح جهان** [۷]

شکل ۳ موقعیت استانداردهای برجسته امنیت اطلاعات را به تصویر کشیده است:






**شکل ۳: موقعیت استانداردهای برجسته امنیت اطلاعات [۷]**

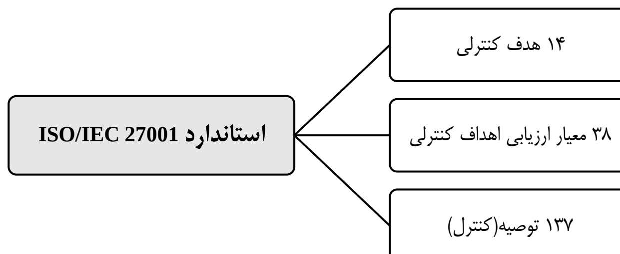
همان‌طور که در شکل ۳ مشاهده می‌شود هر استاندارد در اجرای ISMS نقش و موقعیت خود را دارد، استانداردهایی از جمله ISO/IEC 27001 و BS 7799 بر روی سیستم مدیریت امنیت اطلاعات به‌عنوان دامنه اصلی متمرکز هستند درحالی‌که تمرکز استاندارد PCI-DSS محدود به معاملات کسب‌وکار و کارت هوشمند بوده و پس از آن COBIT و ITIL بر امنیت اطلاعات و ارتباط آن به مدیریت پروژه و مدیر فناوری اطلاعات تمرکز دارد. اشاره به قابلیت استانداردها نشان می‌دهد که ISO/IEC 27001 از چهار استاندارد دیگر به‌ویژه در زمینه ISMS پیشرو است؛ بنابراین استاندارد ISO/IEC 27001 نسبت به چهار استاندارد امنیتی دیگر به‌خوبی شناخته شده و به‌آسانی اجرا می‌شود به همین دلیل موجبات پذیرش آن توسط ذی‌نفعان را فراهم می‌سازد [۷]. مطابق با آخرین آمار منتشرشده از سوی سازمان استاندارد جهانی ایزو تعداد گواهی‌های ISMS صادرشده استاندارد ISO/IEC 27001 هرساله روند صعودی داشته است. در سال ۲۰۱۶ با رشد ۲۱٪+ نسبت به سال ۲۰۱۵ تعداد گواهی‌های صادر شده به ۳۳۲۹۰ گواهینامه معتبر رسیده است [۴]. با توجه به اینکه هدف پژوهش حاضر ارائه یک مدل سلسله مراتبی ممیزی امنیت اطلاعات در سازمان می‌باشد به دلایل زیر استاندارد ISO/IEC 27001 برای ادامه پژوهش انتخاب می‌گردد:

- ✓ استاندارد ISO/IEC 27001 مهم‌ترین و پرمراجعه‌ترین استاندارد مدیریت امنیت اطلاعات است.
- ✓ استاندارد ISO/IEC 27001 زمینه مناسبی برای بهره‌گیری از رویکرد حفاظت سازمانی فراهم کرده است و به تمام سازمان‌ها با هر اندازه، ساختار، فرهنگ سازمانی و هر سطح بلوغی کمک می‌کند تا با پیاده‌سازی و استقرار سیستم مدیریت امنیت اطلاعات فرآیندهای امنیتی خود را متناسب با الزامات خویش به نحو مطلوبی بهبود ببخشند.
- ✓ استاندارد ISO/IEC 27001 می‌تواند توسط مرجع تائید شده ISO مورد ممیزی قرار بگیرد و سازمان‌های مورد تائید موفق به اخذ گواهینامه معتبر شوند.
- ✓ نسبت به سایر استانداردها پوشش کامل‌تری در فرآیندها و کنترل‌های امنیتی دارد.
- ✓ گستردگی استفاده از این استاندارد در سطح جهان قابل توجه است.
- ✓ به دلیل اجرا و پیاده‌سازی آسان‌تر نسبت به استانداردهای دیگر، مقبولیت بهتری توسط ذی‌نفعان دارد.

✓ هرساله تعداد گواهینامه‌های صادر شده استاندارد ISO/IEC 27001 توسط سازمان‌ها رشد صعودی قابل توجهی داشته است.

### ۲-۵- استاندارد ISO/IEC 27001

استاندارد بین‌المللی ISO/IEC 27001 به‌منظور ارائه الزاماتی برای استقرار، پیاده‌سازی، نگهداری و بهبود مستمر یک سیستم مدیریت امنیت اطلاعات تهیه‌شده است. استاندارد ISO/IEC 27001 نمای کلی و واژگان سیستم‌های مدیریت امنیت اطلاعات را توصیف کرده و مرجع خانواده استاندارد مدیریت امنیت اطلاعات شامل ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005 به همراه اصطلاحات و تعاریف مرتبط با آن‌ها است. این استاندارد برای ضمانت انتخاب کنترل‌های امنیتی به‌جا و مناسب برای حفاظت از دارایی‌های اطلاعاتی، طراحی‌شده است. زمانی که یک سازمان موفق به دریافت گواهینامه مربوط به استاندارد ISO/IEC 27001 می‌گردد، به این معنی است که آن سازمان توانسته امنیت را در زمینه اطلاعات خود مطابق با بهترین روش‌های ممکن مدیریت نماید. این استاندارد برای پیاده‌سازی در انواع سازمان‌های دولتی، خصوصی، بزرگ و یا کوچک مناسب است. این استاندارد اظهار می‌دارد که در هر ناحیه، ممیز باید اوضاع کنونی را با توجه به معیارها یا استانداردهای امنیتی که می‌تواند سازمان را به بهترین نحو محافظت کنند ارزیابی نماید [۸]. شکل ۴ ساختار کلی استاندارد ISO/IEC 27001 و شکل ۵ سرفصل‌های کنترلی آن را نمایش می‌دهد.




**شکل ۴: ساختار کلی استاندارد ایزو ۲۷۰۰۱**




**شکل ۵: اهداف کنترلی استاندارد ایزو ۲۷۰۰۱**

**۲-۶- تکنیک دیمتل**

این تکنیک یک روش ارزیابی تصمیم است که در سال ۱۹۷۱ توسط Fonteal و Gabus برای حل مسائل پیچیده تصمیم‌گیری توسعه داده شده است. این روش به‌منظور کشف رابطه علت و معلولی میان معیارها و شناسایی عوامل تأثیرگذار که بیشترین تأثیر را در روند تصمیم‌گیری دارد دنبال می‌شود. [۹]. این تکنیک شامل مراحل زیر می‌باشد:

۱. ساخت ماتریس ارتباط مستقیم بر اساس نظرات خبرگان

ارزیابی روابط میان معیارها (تأثیر یک معیار بر معیار دیگر) بر اساس نظرات خبرگان تحقیق با استفاده از طیف رتبه‌بندی ۰ تا ۴ انجام می‌گردد که در آن ۰ به معنی عدم تأثیرگذاری، ۱ به معنی تأثیر اندک، ۲ به معنی تأثیر متوسط، ۳ به معنی تأثیر زیاد و ۴ به معنی تأثیر بسیار زیاد می‌باشد. در این مرحله برای تشکیل ماتریس ارتباط مستقیم از میانگین نظرات خبرگان استفاده می‌شود:

$$A=\begin{bmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{bmatrix} \qquad (۱)$$

۲. نرمال کردن ماتریس ارتباط مستقیم

ماتریس ارتباط مستقیم با استفاده از روابط زیر نرمال شده و ماتریس N به دست می‌آید:

$$N= VA \qquad (۲)$$

$$V= min\{1/\max_i \sum_{j=1}^{n} a_{ij} \ ,\ 1/\max_j \sum_{i=1}^{n} a_{ij}\} \ ,\ i,j\in\{1,2,\dots,n\} \qquad (۳)$$

۳. محاسبه ماتریس ارتباطات کامل معیارها

بعد از نرمال شدن ماتریس $A$ ماتریس $N$ به دست آمد، ماتریس ارتباطات کامل از طریق رابطه زیر به دست خواهد آمد. در این رابطه I بیانگر ماتریس واحد می‌باشد.

$$Tc=N+N^2+\dots+N^h=N(I-N)^{-1},\ when\ \lim_{h\to\infty} N^h \qquad (۴)$$

۴. تشکیل نگاشت روابط شبکه

به‌منظور تعیین نگاشت روابط شبکه از دو بردار $r$ و $j$ استفاده می‌شود که به ترتیب مجموع ردیف‌ها و ستون‌های ماتریس $T$ می‌باشد که از روابط زیر محاسبه می‌شوند:

$$r = [r_i]n*1 = \left[\sum_{j=1}^{n} t_{ij}\right]_{n*1} \quad (۵)$$

$$d = [d_j]n*1 = \left[\sum_{i=1}^{n} t_{ij}\right]_{1*n} \quad (۶)$$

$r_i$ به معنی مجموع $i$ مین ردیف ماتریس $T$ و نشان‌دهنده مجموع تأثیرات مستقیم و غیرمستقیم معیار $I$ بر دیگر معیارهاست. $dj$ به معنی $j$ امین ستون ماتریس $T$ و نشان‌دهنده مجموع تأثیرات مستقیم و غیرمستقیم است که دیگر معیارها بر معیار $j$ می‌گذارند. شاخص $r_i + d_j$ بیانگر میزان اهمیت (شدت) معیار $i$ ام می‌باشد. شاخص $r_i - d_j$ نشان‌دهنده تأثیرگذاری و یا تأثیرپذیری معیار $i$ می‌باشد. در حالت کلی، چنانچه $r_i - d_j$ مثبت باشد ($i=j$)، معیار $i$ ام جز دسته معیارهای علی یا تأثیرگذار است. چنانچه $r_i - d_j$ منفی باشد ($i=j$)، معیار $i$ام جزء گروه معیارهای تأثیرپذیر است. به همین صورت میزان شاخص $r$ و $d$ را محاسبه می‌نماییم. نمودار سببی بر پایه دو شاخص مذکور قابل ترسیم بوده که به نقشه روابط شبکه معروف است. با توجه به این نقشه می‌توان تصمیم گرفت که چگونه ابعاد و معیارها را می‌توان بهبود داد [۹].

### ۲-۷- تکنیک واسپاس

تکنیک واسپاس (ارزیابی محصول جمع شده با وزن) یکی از روش‌های تصمیم‌گیری چند شاخصه است که در سال ۲۰۱۲ توسط آقای Zavadskas و همکاران در پژوهشی معرفی شد. این روش ترکیبی از دو روش مدل مجموع وزنی و مدل محصول وزنی می‌باشد و نسبت به مدل‌های مستقل از دقت بالاتری برخوردار است [۱۰]. این تکنیک شامل مراحل زیر می‌باشد:

۱. تشکیل ماتریس تصمیم بر اساس معیارها و نظرات خبرگان

۲. نرمال‌سازی ماتریس تصمیم به‌وسیله روش خطی و توسط فرمول زیر:

اگر معیارها دارای نقش مثبت در تصمیم‌گیری باشند از رابطه زیر استفاده می‌کنیم:

$$\bar{x}_{ij} = \frac{x_{ij}}{Max_i\, x_{ij}} \quad (۷)$$

اگر معیارها دارای نقش منفی در تصمیم‌گیری باشند از رابطه زیر استفاده می‌کنیم:

$$\bar{x}_{ij} = \frac{Min_i\, x_{ij}}{x_{ij}} \quad (۸)$$

۳. محاسبه اهمیت نسبی گزینه‌ها بر اساس روش مدل مجموع وزنی:

$$Q_I^{(1)} = \sum_{j=1}^{n} \bar{x}_{ij}\, w_j \quad (۹)$$

۴. محاسبه اهمیت نسبی گزینه‌ها بر اساس روش مدل محصول وزنی:

(۱۰)

$$Q_i^{(2)} = \prod_{j=1}^{n}(\bar{x}_{ij})^{wj}$$

۵. در این گام اهمیت نسبی گزینه i م از طریق فرمول زیر محاسبه می‌شود:

$$Q_i = \lambda\ Q_I^{(1)} + (1-\lambda)\ Q_i^{(2)},\ \lambda = 0, \ldots, 1 \quad (۱۱)$$

در این گام Landa بهینه طبق فرمول زیر محاسبه می‌شود:

$$\lambda = \frac{\sigma^2(Q_i^{(2)})}{\sigma^2\left(Q_i^{(1)}\right) + \sigma^2(Q_i^{(2)})} \quad (۱۲)$$

در معادله‌های فوق $\bar{x}$ ij مقدار نرمال شده $x_{ij}$ و $Max_i\ x_{ij}$ بیشترین مقدار $x_{ij}$ در شاخص j می‌باشد. بدیهی است هر گزینه که مقدار $Q$ بالاتری کسب کند دارای امتیاز بالاتری است [۱۰].

## ۳- یافته‌ها

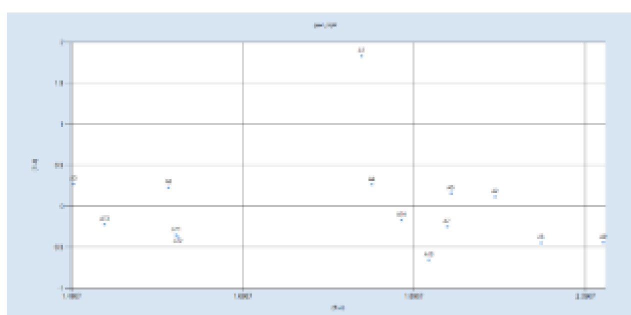
آنچه تاکنون بیان شد نشان داد تا چه حد امنیت اطلاعات برای سازمان مهم بوده و این موضوع یکی از چالش‌های جهانی است. به همین علت استانداردها و به‌روش‌های بسیاری برای ارزیابی امنیت اطلاعات تدوین و ارائه شده‌اند که می‌تواند به سازمان‌ها کمک کند تا سطح امنیت اطلاعات خود را محاسبه کرده، مشکلات و موانعی که در جهت رسیدن به سطح امنیتی مناسب بر سر راه آن‌ها قرار دارد را شناسایی و با توجه به سطحی که در آن قرار دارند با استفاده از تکنیک‌ها و فرآیندهای مناسب برای رسیدن به سطح امنیتی بالاتر گام بردارند. در این مقاله پس از بررسی استانداردهای مختلف در زمینه مدیریت امنیت اطلاعات همان‌طور که در بخش ادبیات نظری بیان شد، استاندارد ISO/IEC 27001 به دلایلی چون گستردگی استفاده، محبوبیت و پیاده‌سازی آسان برای ادامه پژوهش انتخاب گردید. سپس از مطالعه منابع کتابخانه‌ای و استاندارد ISO/IEC 27001 اهداف کنترلی و معیارهای ارزیابی استاندارد ISO/IEC 27001 استخراج شدند. به‌منظور رتبه‌بندی اهداف و معیارهای شناسایی شده با استفاده از ابزار پرسشنامه نظر دوازده تن از خبرگان حوزه فناوری اطلاعات جمع‌آوری شد. بعد از جمع‌آوری داده‌ها از طریق پرسشنامه نظرسنجی از خبرگان و تحلیل اطلاعات گردآوری‌شده دوازده خبره، نتیجه رتبه‌بندی اهداف کنترلی با تکنیک دیمتل و رتبه‌بندی معیارهای ارزیابی با تکنیک واسپاس به‌صورت زیر بیان می‌شود:

**جدول ۱- رتبه‌بندی اهداف کنترلی استاندارد ایزو ۲۷۰۰۱ با استفاده از تکنیک دیمتل**

| اهداف کنترلی | علامت اختصاری | تأثیرگذار/پذیر | R | J | R+J | R-J |
|---|---|---|---|---|---|---|
| خط‌مشی‌های امنیت اطلاعات | A1 | تأثیرگذار | 1.8354 | 0 | 1.8354 | 1.8354 |
| مدیریت دارایی‌ها | A2 | تأثیرگذار | 1.0586 | 0.7886 | 1.8472 | 0.27 |

| R-J | R+J | J | R | تأثیرگذار/پذیر | علامت اختصاری | اهداف کنترلی |
|---|---|---|---|---|---|---|
| 0.1179 | 1.9912 | 0.9366 | 1.0545 | تأثیرگذار | A3 | ساختار امنیت اطلاعات |
| 0.1619 | 1.9399 | 0.889 | 1.0509 | تأثیرگذار | A4 | کنترل دسترسی |
| 0.2307 | 1.6102 | 0.6897 | 0.9205 | تأثیرگذار | A5 | رمزگذاری |
| 0.2755 | 1.4989 | 0.6117 | 0.8872 | تأثیرگذار | A6 | امنیت منابع انسانی |
| -0.1656 | 1.8818 | 1.0237 | 0.8581 | تأثیرپذیر | A7 | انطباق |
| -0.2461 | 1.9355 | 1.0908 | 0.8447 | تأثیرپذیر | A8 | امنیت فیزیکی و محیطی |
| -0.4397 | 2.1174 | 1.2785 | 0.8388 | تأثیرپذیر | A9 | امنیت ارتباطات |
| -0.4466 | 2.0451 | 1.2459 | 0.7993 | تأثیرپذیر | A10 | امنیت عملیات |
| -0.2191 | 1.5352 | 0.8771 | 0.6581 | تأثیرپذیر | A11 | مدیریت تداوم امنیت اطلاعات |
| -0.349 | 1.6189 | 0.9839 | 0.635 | تأثیرپذیر | A12 | روابط تأمین‌کنندگان |
| -0.6505 | 1.914 | 1.2822 | 0.6317 | تأثیرپذیر | A13 | اکتساب، توسعه و نگهداری از سیستم |
| -0.3748 | 1.6211 | 0.9979 | 0.6231 | تأثیرپذیر | A14 | مدیریت رخدادهای امنیت اطلاعات |

با استفاده از دو شاخص *R-J* و *R+J* نمودار سببی به‌صورت زیر ترسیم‌شده و در شکل ۶ نمایش داده شده است:



**شکل ۶: نمودار سببی**

**جدول ۲- رتبه‌بندی معیارهای ارزیابی استاندارد ایزو ۲۷۰۰۱ با استفاده از تکنیک واسپاس**

| WSM | WPM | Q1 | Q2 | Landa | Score | نتیجه |
|---|---|---|---|---|---|---|
| 10.75 | 0.237305 | 0.024531 | 0.001689 | 0.06443 | 6.51000000 | خط‌مشی‌هایی برای امنیت اطلاعات و بازبینی‌های آن |
| 9.75 | 0.059326 | 0.020781 | 0.000106 | 0.005055 | 2.22532557 | الزامات امنیتی سیستم‌های اطلاعاتی |
| 9.25 | 0.037542 | 0.018281 | 4.23E-05 | 0.002308 | 1.43721585 | نقش‌ها و مسئولیت‌های امنیت اطلاعات |
| 10.25 | 0.133484 | 0.022344 | 0.000535 | 0.023364 | 0.91464110 | مسئولیت دارایی‌ها |
| 9.75 | 0.066742 | 0.020469 | 0.000134 | 0.006486 | 0.58018468 | طبقه‌بندی اطلاعاتی |
| 11.25 | 0.421875 | 0.026719 | 0.005339 | 0.166552 | 0.36985064 | مدیریت دسترسی کاربران |
| 10.25 | 0.118652 | 0.022656 | 0.000422 | 0.018301 | 0.23823743 | مدیریت دسترسی به سیستم و برنامه‌ها |
| 11.5 | 0.5625 | 0.027813 | 0.009492 | 0.25445 | 0.15559147 | حفاظت در برابر بدافزارها |
| 11.5 | 0.5625 | 0.027813 | 0.009492 | 0.25445 | 0.15559147 | سیاست در استفاده از کنترل رمزنگاری |
| 7.5 | 0.002086 | 0.0125 | 1.31E-07 | 1.04E-05 | 0.08657785 | رویه‌های عملیاتی و مسئولیت‌ها |
| 8.25 | 0.008343 | 0.014844 | 2.09E-06 | 0.000141 | 0.03465566 | ملاحظات ممیزی سیستم‌های اطلاعاتی |
| 6.5 | 0.000309 | 0.009688 | 2.86E-09 | 2.96E-07 | 0.01506535 | انطباق با الزامات قانونی و قراردادی |
| 7.5 | 0.001854 | 0.012813 | 1.03E-07 | 8.05E-06 | 0.00393243 | بازنگری‌های امنیت اطلاعات |
| 10.5 | 0.177979 | 0.023438 | 0.00095 | 0.038966 | 0.00391313 | امنیت اطلاعات در مدیریت پروژه‌ها |
| 9.75 | 0.052734 | 0.021094 | 8.34E-05 | 0.003939 | 0.00094211 | گزینش |
| 6.25 | 0.000154 | 0.009219 | 7.16E-10 | 7.77E-08 | 0.00062492 | نیازمندی‌های تجاری کنترل دسترسی |
| 10.25 | 0.079102 | 0.023281 | 0.000188 | 0.007998 | 0.00041552 | واقعه‌نگاری و پایش |
| 5 | 8.58E-06 | 0.00625 | 2.21E-12 | 3.54E-10 | 0.00041518 | تجهیزات |

| WSM | WPM | Q1 | Q2 | Landa | Score | نتیجه |
|---|---|---|---|---|---|---|
| 7.75 | 0.002197 | 0.014219 | 1.45E-07 | 1.02E-05 | 0.00020689 | کنترل نرم‌افزارهای عملیاتی |
| 10.75 | 0.237305 | 0.024531 | 0.001689 | 0.06443 | 0.00013775 | پشتیبان گیری |
| 7 | 0.000618 | 0.011563 | 1.15E-08 | 9.91E-07 | 0.00006113 | امنیت اطلاعات در روابط با تأمین‌کنندگان |
| 11 | 0.28125 | 0.025938 | 0.002373 | 0.083822 | 0.00006112 | انتقال اطلاعات |
| 8.25 | 0.005562 | 0.015469 | 9.28E-07 | 6.00E-05 | 0.00003054 | مدیریت و بهبود رخدادهای امنیت اطلاعات |
| 7.25 | 0.000927 | 0.012344 | 2.58E-08 | 2.09E-06 | 0.00001526 | تداوم امنیت اطلاعات |
| 10.75 | 0.237305 | 0.024531 | 0.001689 | 0.06443 | 0.00000763 | در حین خدمت |
| 8.5 | 0.007416 | 0.016563 | 1.65E-06 | 9.96E-05 | 0.00000382 | خاتمه اشتغال |
| 10.75 | 0.210938 | 0.024844 | 0.001335 | 0.05099 | 0.00000382 | نواحی امن |
| 6.5 | 0.000275 | 0.01 | 2.26E-09 | 2.26E-07 | 0.00000095 | مدیریت رسانه |
| 11 | 0.316406 | 0.025625 | 0.003003 | 0.104909 | 0.00000095 | کنترل شبکه |
| 8.75 | 0.011124 | 0.017344 | 3.71E-06 | 0.000214 | 0.00000095 | امنیت در فرآیندهای توسعه و پشتیبانی |
| 3.75 | 3.58E-07 | 0.003594 | 3.84E-15 | 1.07E-12 | 0.00000048 | استفاده از تلفن همراه |
| 5.25 | 1.72E-05 | 0.006719 | 8.84E-12 | 1.32E-09 | 0.00000038 | ارتباط با مقامات |
| 4 | 7.15E-07 | 0.004063 | 1.53E-14 | 3.78E-12 | 0.00000038 | تماس با گروه‌های خاص |
| 5.25 | 8.58E-06 | 0.007656 | 2.21E-12 | 2.89E-10 | 0.00000024 | دور کاری |
| 8 | 0.003708 | 0.014688 | 4.12E-07 | 2.81E-05 | 0.00000024 | مدیریت آسیب‌پذیری فنی |
| 5.75 | 6.87E-05 | 0.007656 | 1.41E-10 | 1.85E-08 | 0.00000024 | افزونگی |
| 7 | 0.000695 | 0.01125 | 1.45E-08 | 1.29E-06 | 0.00000012 | مدیریت تحویل خدمات تامین‌کنندگان |
| 5.25 | 2.29E-05 | 0.006406 | 1.57E-11 | 2.45E-09 | 0.00000006 | داده‌های آزمون |







## ۴- بحث و نتیجه‌گیری

هر پژوهشی با ارائه ایده‌ها و پیشنهادهای صحیح و متناسب با حیطه موضوعی موردنظر انجام می‌شود تا بتواند به شکل نظری و یا کاربردی مسئله و مشکلی را حل کند یا راه‌حل‌های فعلی را بهبود ببخشد. پژوهش حاضر نیز در راستای بهبود ارزیابی امنیت اطلاعات در سازمان‌ها شکل‌گرفته است. این پژوهش با نگاهی واقع‌گرا به عوامل مؤثر در ارزیابی امنیت اطلاعات به رتبه‌بندی و تعیین اولویت اهداف و معیارهای ارزیابی امنیت اطلاعات استاندارد بین‌المللی ایزو ۲۷۰۰۱ پرداخته است. به‌منظور رتبه‌بندی و تعیین اولویت اهداف از تکنیک دیمتل و به‌منظور رتبه‌بندی معیارها از روش قدرتمند واسپاس بهره برده شده است. طبق نتایج به‌دست‌آمده «خط‌مشی‌های امنیت اطلاعات» و «اکتساب، توسعه و نگهداری از سیستم» به ترتیب تأثیرگذارترین عامل و تأثیرپذیرترین عامل در تحقق امنیت اطلاعات سازمان بوده و «خط‌مشی‌هایی برای امنیت اطلاعات و بازبینی‌های آن» و «داده‌های آزمون» به ترتیب پراهمیت‌ترین معیار و کم‌اهمیت‌ترین معیار ارزیابی امنیت اطلاعات می‌باشد. تاکنون در هیچ‌یک از تحقیقات داخلی و خارجی انجام شده میزان اهمیت این اهداف متفاوت از هم در نظر نگرفته شده است. پیشنهاد می‌گردد در ممیزی امنیت اطلاعات و محاسبه سطح امنیت اطلاعات سازمان تأثیر رتبه‌بندی اهداف و معیارها در نظر گرفته شود.

## مراجع

[1] Atymtayeva, Bortsova, Inoue, & Kozhakhmet, (2012). Methodology and ontology of expert system for information security audit. Paper presented at the Soft Computing and Intelligent Systems (SCIS) and 13th International Symposium on Advanced Intelligent Systems (ISIS), 2012 Joint 6th International Conference on, 116(8), 365-375.

[2] Palaniapan, Sh. Ahmad, R. Zolait, A. & Sedek, M. (2017). Integrating information quality dimensions into information security risk management (ISRM). Information Security and Applications. 36(6), 1-10.

[۳] بازرگانی، مهدی. سلیمانی، حسین. عمادی، پیمان. پیاده‌سازی سیستم مدیریت امنیت اطلاعات با ارزیابی مدل کنترل دسترسی. (۱۳۹۴). کنفرانس بین‌المللی پژوهش‌های کاربردی در فناوری اطلاعات، کامپیوتر و مخابرات (ص ص ۱۴۱-۱۳۵)

[4] ISO/IEC 27000. (2013). Information technology, Security techniques. Information security management systems. Retrieved from :https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

[5] Wallhoff, J. (2004). Combining ITIL with COBIT and ISO/IEC 17799: 2000. Scillani Information AB. Retrieved from http://www.scillani.com.

[6] Olzak T (2013) Insider threats: implementing the right controls. TechRepublic, Originally published 21 Feb 2013. Retrieved from http://www.techrepublic.com/blog/it-security/insider-threats implementing-the-right-controls/.

[7] Almunawar, M. Chee, Y. Susanto, H. (2015). Information Security Management System Standards:A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences. 11(05), 121-128

[8] Chang, L.Y. & Lee, Z.J. (2013). Applying fuzzy expert system to information security risk Assessment-A case study on an attendance system. Paper presented at the Fuzzy Theory and Its Applications (iFUZZY), 2013 International Conference on, 54(5), 45-57.

[9] Deepak, S. Sushant, T. Sarat, Kumar. Dematel approach for analyzing the critical factor in remanufacturing process. Materials Today: Proceedings 5 (2018) 18568–18573

[10] Zavadskas EK, Turskis Z, Antucheviciene J, Zakarevicius A. Optimization of Weighted Aggregated Sum Product Assessment. Electronics and Electrical Engineering. 2012;122(6):3-6.